Section I:

AMENDMENT UNDER 37 CFR §1.121 to the CLAIMS

Claim 1 (previously amended):

A method for detecting possible security violations and issues in a computer system related to user ID substituting and switching, said computer system having a log of user ID substitutions and switches, said method comprising the steps of:

providing a set of rules in a computer-readable alarm conditions file, said rules defining conditions of user ID substitutions and switches which are to be considered possible security issues, at least one of which rules is a rule besides a rule defining a number of failed user switches in a specified time period beginning at a first failed attempt, wherein said number is greater than 1;

providing a process adapted to access said alarm conditions file, and to evaluate said log of user ID substitutions and switches according to said set of rules;

evaluating said log of user ID substitutions and switches to find any entries in said log which meet one or more defined conditions in said set of rules; and

outputting an alert responsive to finding one or more log entries which meet said conditions.

Claim 2 (original):

The method as set forth in Claim 1 wherein said step of providing a process adapted to evaluate said log comprises configuring a script to periodically execute by a CRON daemon in a system having a UNIX-like operating system.

Claim 3 (original):

The method as set forth in Claim 1 wherein said step of providing a process adapted to evaluate said log comprises configuring a process to periodically execute by a CRON daemon in a system having a UNIX-like operating system.

Claim 4 (original):

The method as set forth in Claim 1 wherein said step of evaluating said log of user ID substitutions and switches comprises evaluating a SULOG file in a system having a UNIX-like operating system.

Claim 5 (previously amended):

The method as set forth in Claim 1 wherein said rules comprise at least one rule including an electronic mail address to which alert messages should be sent, and wherein said step of outputting an alert comprises sending an electronic message to a predetermined electronic mail address as defined in a rule in said alarm conditions file.

Claim 6 (previously amended):

A computer-readable medium having stored therein program code for detecting possible security violations and issues in a computer system related to user ID substituting and switching, said computer system having a log of user ID substitutions and switches, said program code when executed by a computer system causing the computer system to perform the steps of:

providing a set of rules in a computer-readable alarm conditions file, said rules defining conditions of user ID substitutions and switches which are to be considered possible security issues, at least one of which rules is a rule besides a rule defining a number of failed user switches in a specified time period beginning upon a first failed attempt, wherein said number is greater than 1;

accessing said alarm conditions file;

evaluating said log of user ID substitutions and switches to find any entries in said log which meet one or more defined conditions in said set of rules; and

outputting an alert responsive to finding one or more log entries which meet said conditions.

Claim 7 (original):

The computer readable medium as set forth in Claim 6 wherein said program code for performing the step of evaluating said log comprises program code for configuring a script to periodically execute by a CRON daemon in a system having a UNIX-like operating system.

Claim 8 (original):

The computer readable medium as set forth in Claim 6 wherein said program code for performing the step of evaluating said log comprises program code for configuring a process to periodically execute by a CRON daemon in a system having a UNIX-like operating system.

Claim 9 (original):

The computer readable medium as set forth in Claim 6 wherein said program code for performing the step of evaluating said log of user ID substitutions and switches comprises program code for evaluating a SULOG file in a system having a UNIX-like operating system.

Claim 10 (previously amended):

The computer readable medium as set forth in Claim 6 wherein said rules comprise at least one rule including an electronic mail address to which alert messages should be sent, and wherein said program code for performing the step of outputting an alert comprises program code for sending an electronic message to an electronic mail address as defined in a rule in said alarm conditions file.

Claim 11 (currently amended):

A system for detecting possible security violations and issues in a multi-user computer related to user ID substituting and switching, said multi-user computer having a log of user ID substitutions and switches, said system comprising:

a hardware platform adapted to performing computing tasks with electronic circuitry, software, or both;

a set of rules in ~~a computer-readable~~ an alarm conditions file readable by said hardware platform, said rules defining conditions of user ID substitutions and switches which are to be considered possible security issues, at least one of which rules is a rule besides a rule defining a number of failed user switches in a specified time period beginning from a first failed attempt, wherein said number is greater than 1;

a log evaluator for accessing said alarm conditions files in cooperation with said hardware platform, and for evaluation said log of user ID substitutions and switches to find any entries in said log which meet one or more defined conditions in said set of rules; and

an alert output for outputting an alert responsive to finding one or more log entries which meet said conditions.

Claim 12 (original):

The system as set forth in Claim 11 further comprising a scheduler for periodically operating said log evaluator.

Claim 13 (original):

The system set forth in Claim 12 wherein said scheduler comprises a CRON daemon and said log evaluator comprises a script in a multi-user computer having a UNIX-like operating system.

Claim 14 (original):

The system as set forth in Claim 12 wherein said scheduler comprises a CRON daemon and said evaluator comprises an executable UNIX process in a multi-user computer having a UNIX-like operating system.

Claim 15 (original):

The system as set forth in Claim 11 wherein said evaluator is adapted to evaluate an SULOG file in a multi-user computer system having a UNIX-like operating system.

Claim 16 (previously amended):

The system as set forth in Claim 11 wherein said rules comprise at least one rule including an electronic mail address to which alert messages should be sent, and wherein said alert output comprises a transmitter for an electronic message to said electronic mail address.

Claim 17 (previously added):

The method as set forth in Claim 1 wherein said alarm conditions file comprises a rule to generate an alert upon any user attempting to switch to a specific user ID defined by said rule.

Claim 18 (previously added):

The method as set forth in Claim 17 wherein said specific user ID comprises a root ID.

Claim 19 (previously added):

The method as set forth in Claim 1 wherein said alarm conditions file comprises a rule to generate an alert upon any user attempting to switch to another user ID between certain hours of system operation.